METHOD FOR GENERATING/REGENERATING A CIPHER KEY FOR A CRYPTOGRAPHIC METHOD

Publication number:	WO0108347 (A1)
Publication date:	2001-02-01
Inventor(s):	SCHWENK JOERG [DE]
Applicant(s):	DEUTSCHE TELEKOM AG [DE]; SCHWENK JOERG [DE
international:	H04L9/08; H04L9/08; (IPC1-7): H04L9/08
Application number:	WO2000EP06387 20000706
Priority number(s):	DE19991035285 19990727

Abstract of **WO 0108347 (A1)**

The invention relates to a method for generating/regenerating a cipher key for a cryptographic method, whereby a cipher key and a public key are created from a random number (seed) according to a predetermined deterministic method. According to said method, the seed is created only on the user side through the use of values which are only known to the user. Regeneration information appropriate to the seed regeneration, which allows for the seed to be derived in a deterministic manner from the confidence station through a combination with information known only to said confidence station, is created on the user side and stored in a lossproof manner. In the event of loss of the cipher key, the seed is reproduced on the confidence station side by combining the regeneration information with secrete information.